RED TEAM OPERATIONS – DEVELOPMENT PT.1

Joas Antonio

WARNING

Slide made for a friend with medium grade autism, he is a big fan of anime and comics and I added some characters to help him in his development

WHAT IS RED TEAM?

The Red Team is formed with the objective of carrying out cyberattack tests in the company. We are talking about professionals with high knowledge about the main threats and attacks that exist, being able to simulate attempts to penetrate the network and / or systems.As a result, they are able to identify vulnerabilities and, consequently, eliminate them.

WHAT IS RED TEAM? 2

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization's overall security to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization's security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

WHAT IS RED TEAM? 3

The Red Team concept requires a different approach from a typical security testing and relies heavily on well-defined TTPs, which are critical to successfully emulating a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist. Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate them. This book will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing.

RED TEAM SPECIFIC GOALS

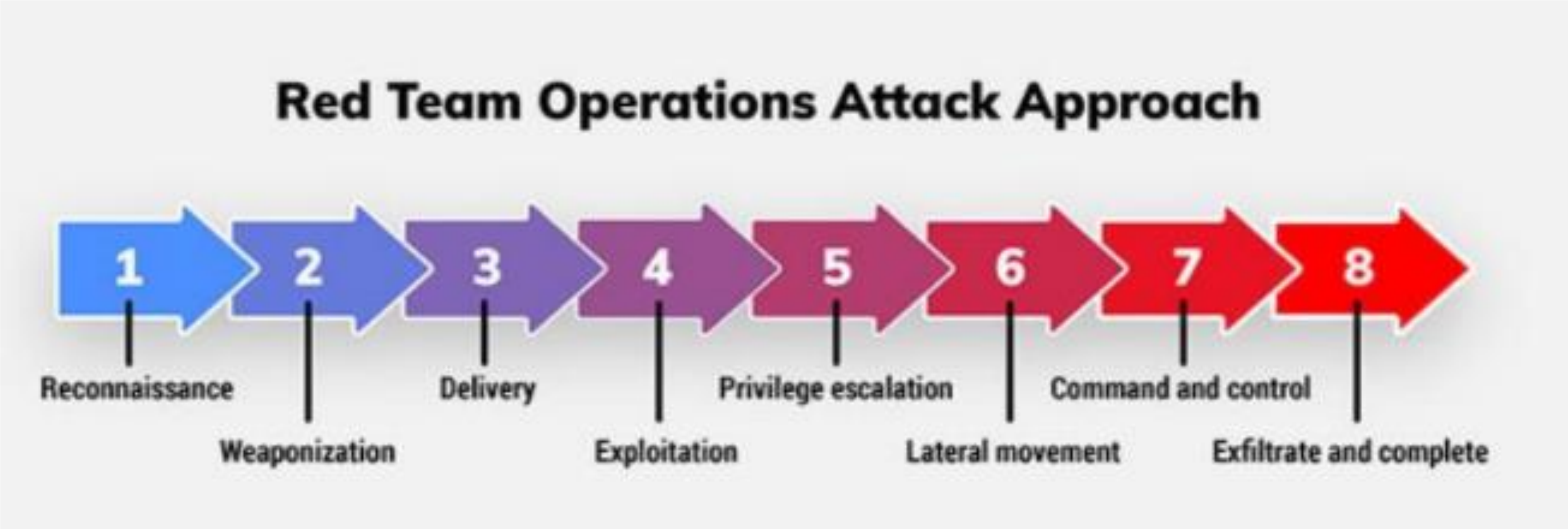
These goals may include compromising an application or network, stealing data, emulating a specific target, measuring the effectiveness of technical defenses, measuring the effectiveness of a security team, etc. The vulnerabilities and weaknesses identified during an assessment may need to be addressed and mitigated, but this is not the focus of Red Teaming. Red Teaming focuses on the bigger picture by providing insight into a target's detection and response capabilities. It gives understanding Mean-Time to Detect (MTTD) and Mean-Time to Recover (MTTR) from individual breaches. It exercises the relationship between its incident response and threat hunting teams by testing network defenders and their tools in ways that cannot be achieved through traditional threat intelligence, literature, or structured testing.

RED TEAM SPECIFIC GOALS 2

Measuring the effectiveness of the people, processes, and technology used to defend a network

When a Red Team uses real-world attack techniques against a target's production network, the extent of the organization's defenses are challenged. For example, an engagement has the goal of stealing critical data from a target. A targeted phishing attack tests the end user's willingness to participate in an attack. The payload of the attack tests the network and host defenses against the delivery of malware and ultimately against code execution. If the attack does trigger a defensive control, the response measures the defender's actions in identifying, responding, or stopping the attack. Red teaming provides a means to measure security operations as a whole and not only focus on technical controls.

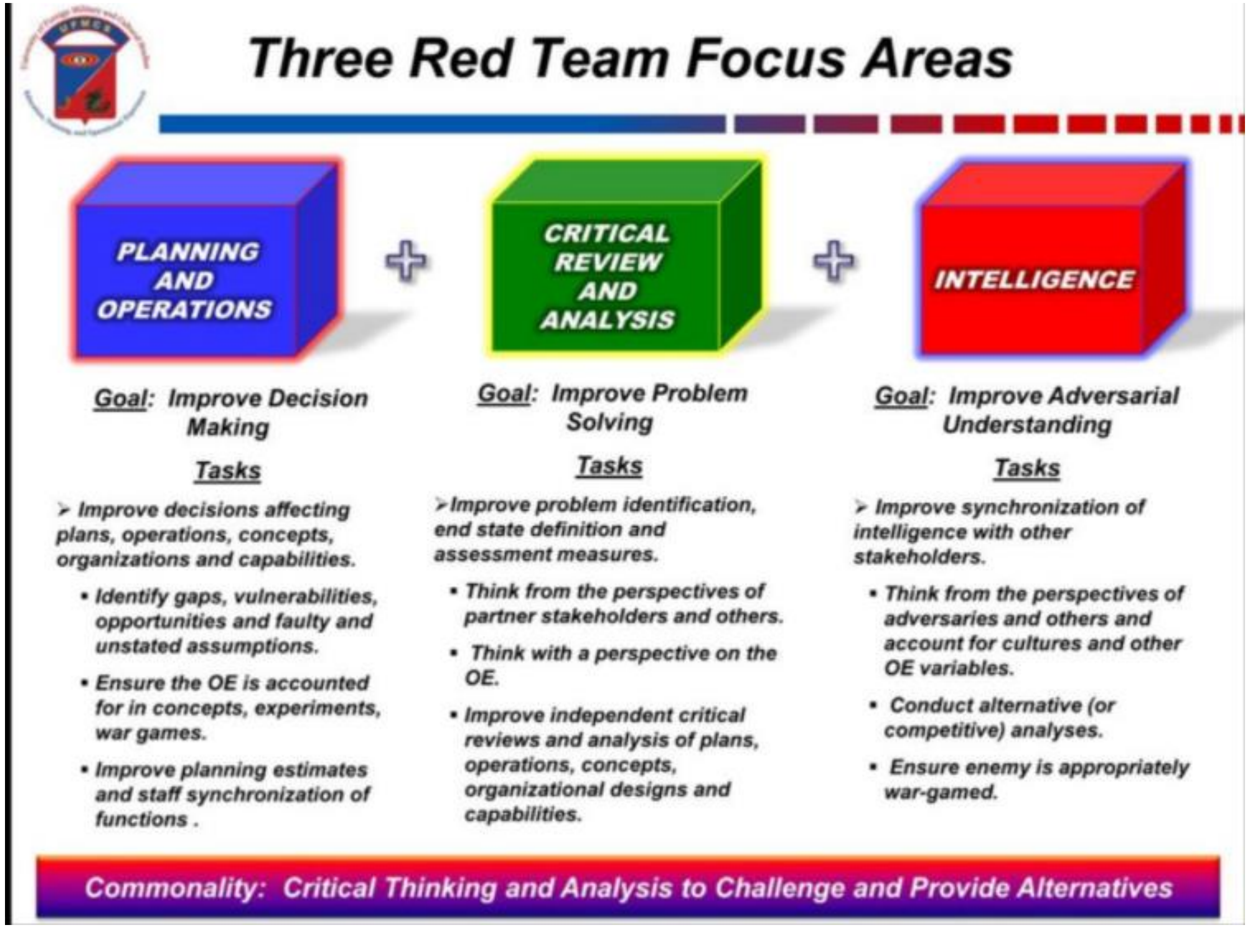
Red Team Operations Attack Approach



Red Team Operations Attack Approach

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Privilege escalation
6. Lateral movement
7. Command and control
8. Exfiltrate and complete

Three Red Team Focus area



Three Red Team Focus Areas

PLANNING AND OPERATIONS + **CRITICAL REVIEW AND ANALYSIS** + **INTELLIGENCE**

PLANNING AND OPERATIONS

Goal: Improve Decision Making

Tasks

➢ Improve decisions affecting plans, operations, concepts, organizations and capabilities.

- Identify gaps, vulnerabilities, opportunities and faulty and unstated assumptions.
- Ensure the OE is accounted for in concepts, experiments, war games.
- Improve planning estimates and staff synchronization of functions .

CRITICAL REVIEW AND ANALYSIS

Goal: Improve Problem Solving

Tasks

➢Improve problem identification, end state definition and assessment measures.

- Think from the perspectives of partner stakeholders and others.
- Think with a perspective on the OE.
- Improve independent critical reviews and analysis of plans, operations, concepts, organizational designs and capabilities.

INTELLIGENCE

Goal: Improve Adversarial Understanding

Tasks

➢ Improve synchronization of intelligence with other stakeholders.

- Think from the perspectives of adversaries and others and account for cultures and other OE variables.
- Conduct alternative (or competitive) analyses.
- Ensure enemy is appropriately war-gamed.

Commonality: Critical Thinking and Analysis to Challenge and Provide Alternatives

Red Team Operator (RTO)

Red Team operators are the individuals who execute the actions required for an engagement to meet the goals. Each Red Team operator complies with all Red Team policies and regulations under the direction of the Red Team Lead. In general, the operator:

- Executes engagement requirements as directed Complies with all laws, regulations, policies, programs and Rules of Engagement Implements the team's operational methodology and TTPs
- Identifies and has input to target environment deficiencies Researches and develops new exploit and tests tools for functionality
- Performs Open Source Intelligence as required for the engagement Identifies and assesses actions that reveal system vulnerabilities and capabilities Assists the Red Team Lead in the development of the final engagement report
- Performs physical assessment support under the direction of Red Team Lead Executes operational impacts as approved by the ECG

Red Team Lead

A Red Team should have a lead for each engagement. The lead may perform the role of the action officer, the engagement lead, an operator, the customer interface, and, often, an analyst. In general, the Red Team lead:

- Provides overall direction and guidance for the team
- Provides information and research data for all laws, regulations, policies, programs, and operations
- Provides oversight for operational planning and execution
- Coordinates with each of the roles within the Red Team engagement
- Plans and manages the budget, personnel, and equipment
- Provides oversight for the team calendar
- Provides information related to engagements, capabilities, technology, and trends
- Provisions training and personnel development requirements
- Performs a budget analysis, including equipment and travel Identifies technical research and development directions

by Red Team Development and Operations

Rules of Engagement (ROE)

The Rules of Engagement establish the responsibility, relationship, and guidelines between the Red Team, the network owner, the system owner, and any stakeholders required for engagement execution.

This document contains all agreed-upon rules for an engagement, should be a signed official

agreement of all parties involved, is used as the formal agreement that authorizes the engagement

actions, and should be treated as law. The ROE governs the entire process of a Red Team engagement and must be adhered to during the execution. Violation of the ROE can put a target organization or engagement operators at risk. The seriousness of the ROE must not be taken lightly. All parties must approve any deviation from the rules established in the ROE before execution.

by Red Team Development and Operations

TTP’s

- Tactics, techniques and procedures (TTPs) are the “patterns of activities or methods associated with a specific threat actor or group of threat actors.”
- Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks.
- Top threats facing an organization should be given priority for TTP maturation. Smaller organizations may benefit strategically by outsourcing research and response.

TTPs help to establish attribution to a foreign nation-state adversary, aiding in maturation of what they’re after. For example, the goal could be to gather policy and government-based classified information of interest for cyberwarfare interests. Potential targets are also identified based upon former targets seen in the campaign as well as potential future targets (e.g. policy related staff responsible for areas of Asia). TTPs also help to identify a common vector of attack – email with an Office attachment containing a first stage and payload, such as a downloader. This helps position for ongoing attacks from the campaign, such as reviewing and changing policy related to Windows Data Execution Prevention (DEP); use of Sandboxie as a virtualized application layer for the endpoint for opening suspect files; a review of possible endpoint protection solutions, and so forth. This hyper-focus on known and potential campaign targets helps IT and security staff proactively harden against attacks and minimize damage (should an incident occur) through threat hunting exercises and further forensics investigation. ***by OPTIV***

C2 FRAMEWORK

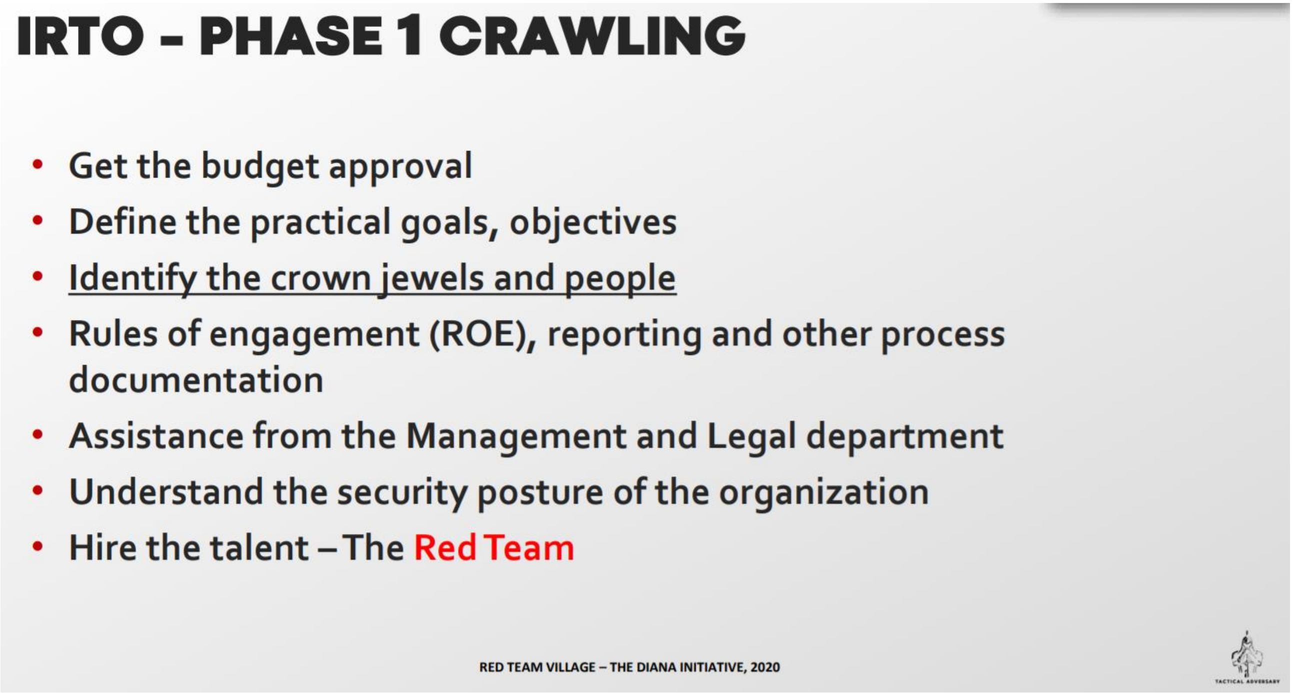
A C2 framework provides red team operators with a means of interacting with compromised systems and leveraging post-exploitation tools to further their engagements. The most useful frameworks not only have features built-in but also allow operators to bring their own custom tooling into the framework.

One of the most damaging attacks, guaranteed by DNS, is accomplished through command and control, also called C2 or C&C. The attacker starts by infecting a computer, which may be behind a firewall. this can be done in several ways:
− Through a phishing email that tricks the user into following a link to a malicious or open website
an attachment that executes malicious code.
− Through security holes in browser plug-ins.
− Through other infected software.
Once communication is established, an infected machine sends a signal to the server of the invader, see your next instruction. Infected computer executes server commands
C2 attacker and may install additional software. The attacker now has full control of the victim and can run any code. Malicious code usually spreads to more computer, creating a botnet.

Red Team Infraestructure

When designing a Red Team infrastructure that needs to withstand an active response or last for a long-term involvement (weeks, months, years), it is important to segregate each asset based on in the function. This provides resiliency and agility against Blue Team when campaign assets began to be detected. Per For example, see a phishing assessment email for identification, the Red Team will only create a new SMTP server and server payload hosting instead of a server setup entire team.

RTO – Phase 1

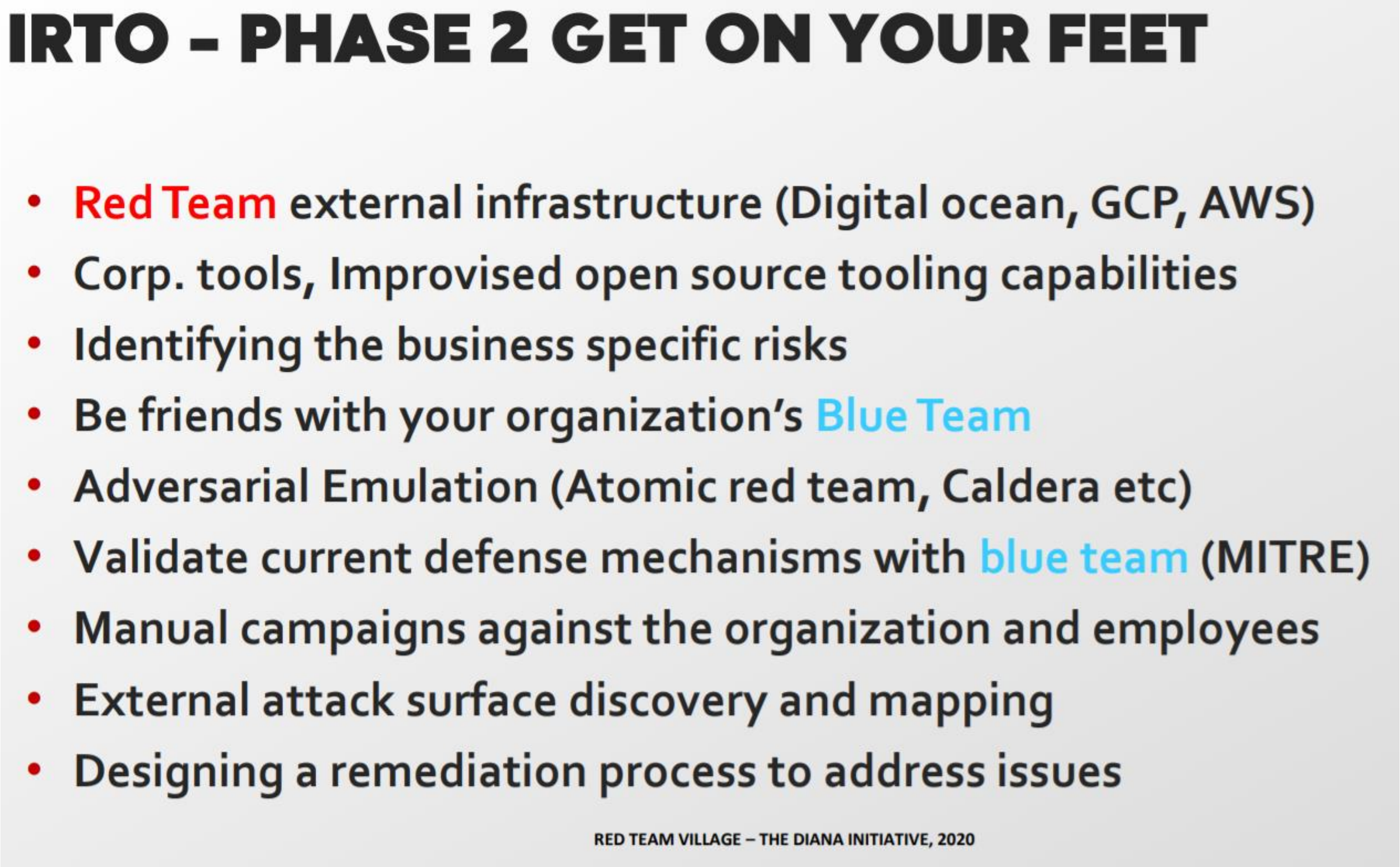


IRTO - PHASE 1 CRAWLING

- Get the budget approval
- Define the practical goals, objectives
- Identify the crown jewels and people
- Rules of engagement (ROE), reporting and other process documentation
- Assistance from the Management and Legal department
- Understand the security posture of the organization
- Hire the talent – The Red Team

RED TEAM VILLAGE – THE DIANA INITIATIVE, 2020

RTO – Phase 2

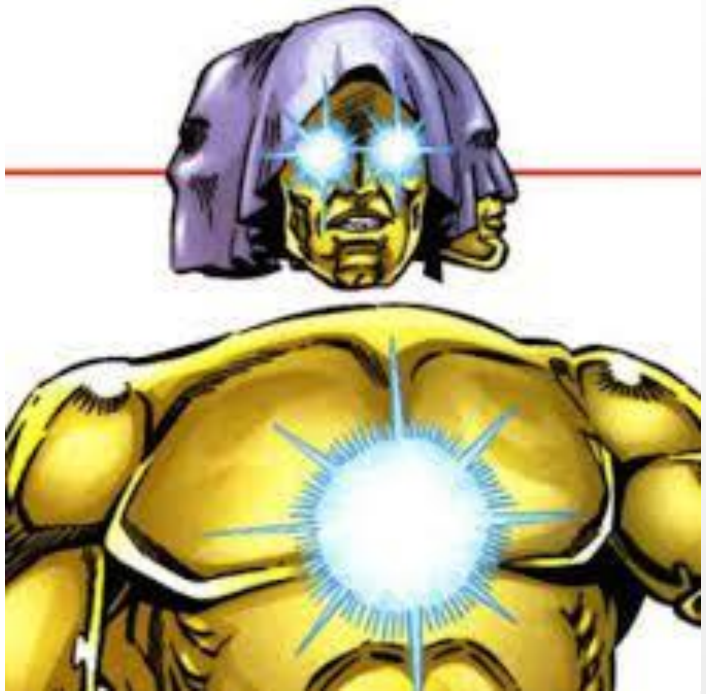


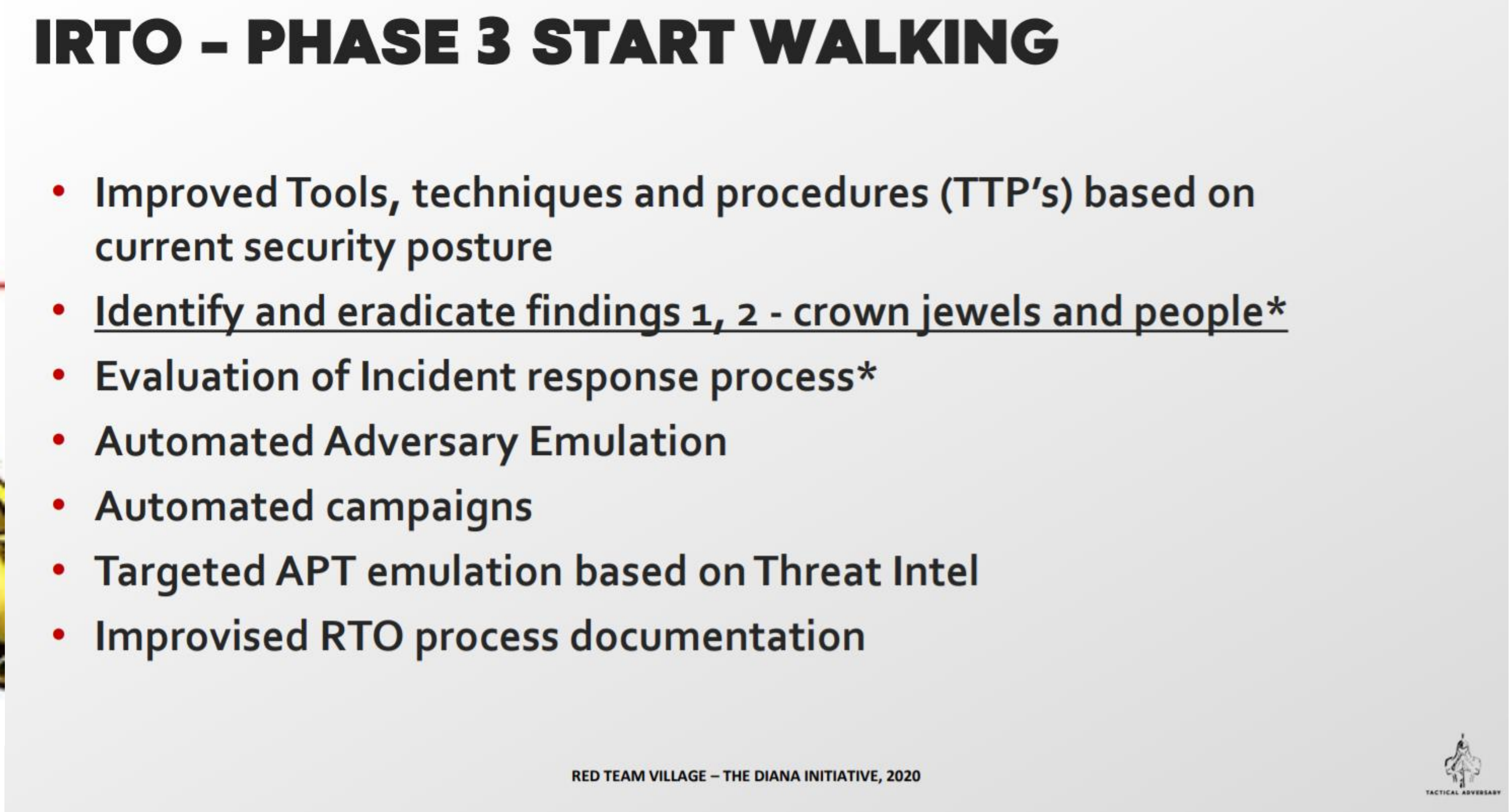
IRTO - PHASE 2 GET ON YOUR FEET

- Red Team external infrastructure (Digital ocean, GCP, AWS)
- Corp. tools, Improvised open source tooling capabilities
- Identifying the business specific risks
- Be friends with your organization's Blue Team
- Adversarial Emulation (Atomic red team, Caldera etc)
- Validate current defense mechanisms with blue team (MITRE)
- Manual campaigns against the organization and employees
- External attack surface discovery and mapping
- Designing a remediation process to address issues

RED TEAM VILLAGE – THE DIANA INITIATIVE, 2020

RTO – Phase 3



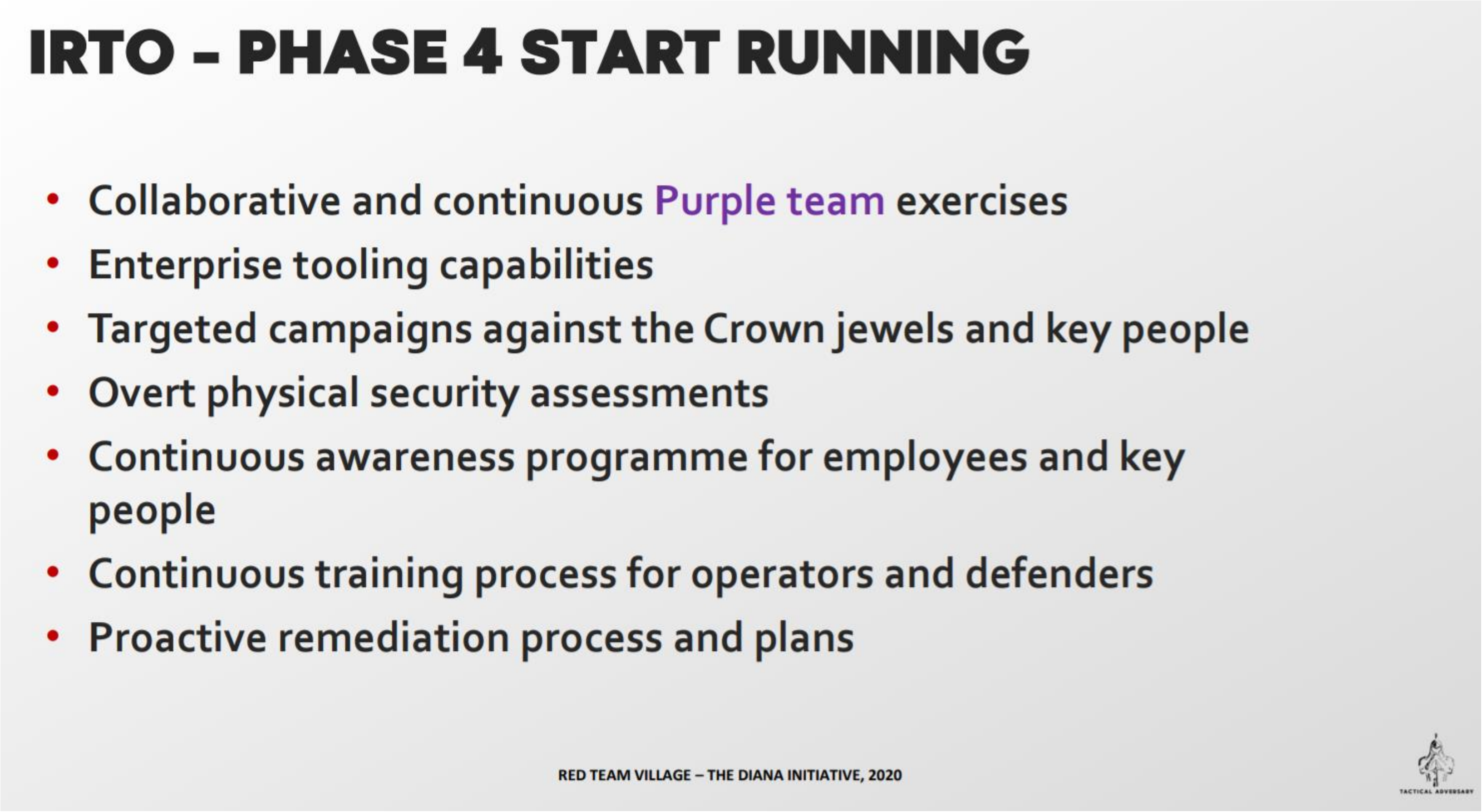


IRTO - PHASE 3 START WALKING

- Improved Tools, techniques and procedures (TTP's) based on current security posture
- Identify and eradicate findings 1, 2 - crown jewels and people*
- Evaluation of Incident response process*
- Automated Adversary Emulation
- Automated campaigns
- Targeted APT emulation based on Threat Intel
- Improvised RTO process documentation

RED TEAM VILLAGE – THE DIANA INITIATIVE, 2020

RTO – Phase 4

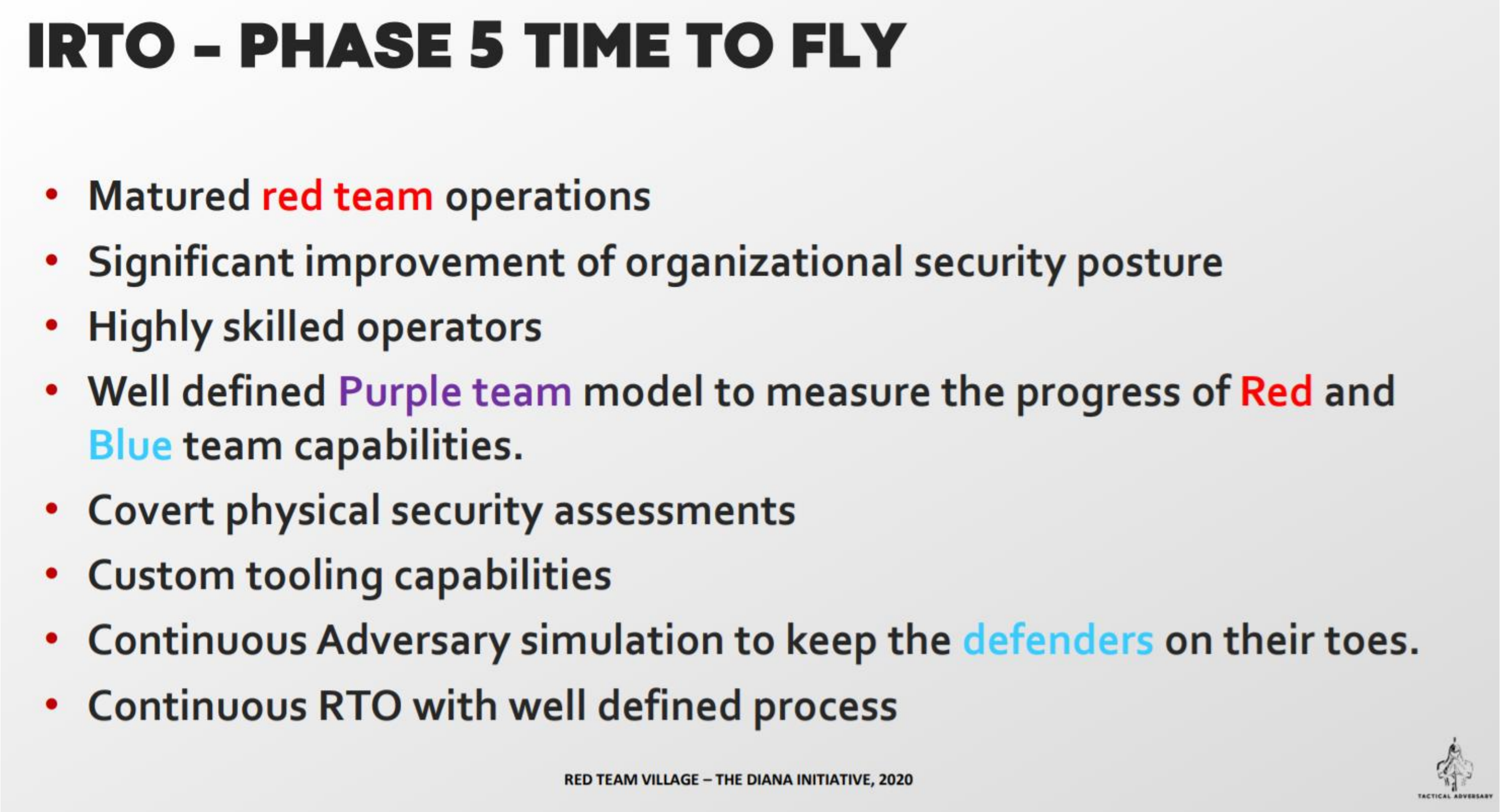


IRTO - PHASE 4 START RUNNING

- Collaborative and continuous Purple team exercises
- Enterprise tooling capabilities
- Targeted campaigns against the Crown jewels and key people
- Overt physical security assessments
- Continuous awareness programme for employees and key people
- Continuous training process for operators and defenders
- Proactive remediation process and plans

RED TEAM VILLAGE – THE DIANA INITIATIVE, 2020

RTO – Phase 5



IRTO - PHASE 5 TIME TO FLY

- Matured red team operations
- Significant improvement of organizational security posture
- Highly skilled operators
- Well defined Purple team model to measure the progress of Red and Blue team capabilities.
- Covert physical security assessments
- Custom tooling capabilities
- Continuous Adversary simulation to keep the defenders on their toes.
- Continuous RTO with well defined process

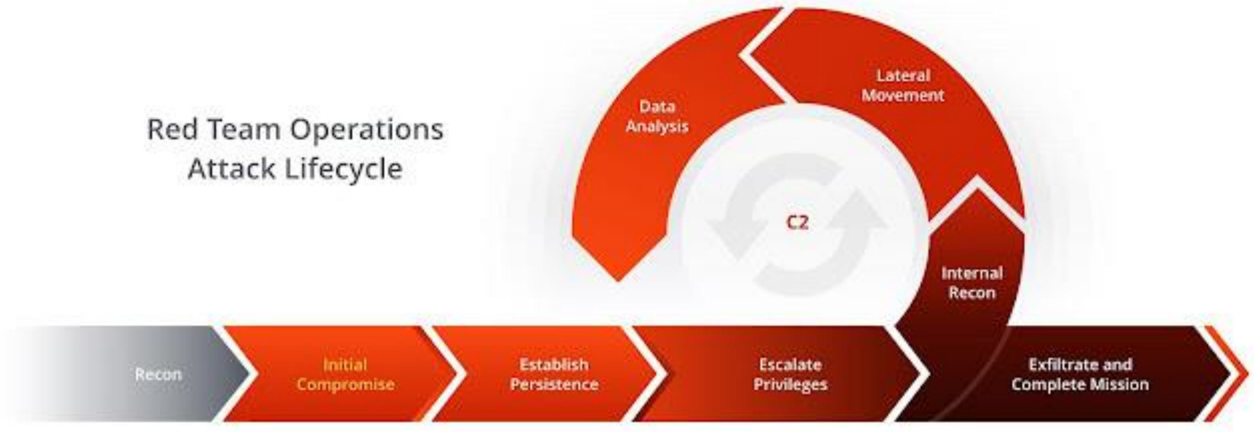
RED TEAM VILLAGE – THE DIANA INITIATIVE, 2020

Threat Emulation

Threat Emulation is the process of mimicking the TTPs of a specific threat. A Red Team performs threat emulation by acting as a representative threat. Threats of any variety can be emulated.

This can include: Zero-day or custom attacks Script kiddie to advanced threat Emulation of specific threat tools or techniques (botnets, DDOS, ransomware, specific malware, APT, etc.)

Red Team Engagement



Red Team Engagements are an effective demonstration of tangible risk posed by an APT (Advanced Persistent Threat). The assessors are instructed to compromise predetermined assets, or “flags,” using means that a malicious actor might utilize in a legitimate attack. These comprehensive, complex security assessments are best suited for companies looking to improve a maturing security organization.

Red Team Engagement - Process

Engagement Planing

Engagement Execution

Engagement Culmination

Engagement Reporting

https://rhinosecuritylabs.com/assessment-services/red-team-engagement/

Red Team Practical

https://github.com/hfiref0x/UACME
https://github.com/SecWiki/windows-kernel-exploits
https://github.com/PowerShellMafia/PowerSploit
https://github.com/rsmudge/ElevateKit
https://github.com/rasta-mouse/Sherlock
https://github.com/0xbadjuju/Tokenvator
https://github.com/gentilkiwi/mimikatz/wiki
https://github.com/ZeroPointSecurity/
https://www.ired.team/offensive-security/lateral-movement/t1047-wmi-for-lateral-movement
https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f
https://redcanary.com/blog/lateral-movement-winrm-wmi/
https://github.com/Mr-Un1k0d3r/PowerLessShell
https://github.com/byt3bl33d3r/CrackMapExec
https://github.com/vysecurity/ANGRYPUPPY

Red Team Practical 2

https://github.com/BloodHoundAD/SharpHound
https://github.com/api0cradle/LOLBAS
https://www.cobaltstrike.com/blog/whats-the-go-to-phishing-technique-or-exploit/
https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0
https://github.com/FSecureLABS/C3
https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88
https://adsecurity.org/?p=230
https://github.com/blackc03r/OSCP-Cheatsheets/blob/master/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets.md
https://github.com/bryant-treacle/Kerberos_Golden_Ticket_Finder
https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets

Red Team Practical 3

https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync
https://github.com/carlospolop/hacktricks/blob/master/windows/active-directory-methodology/dcsync.md
https://github.com/shellster/DCSYNCMonitor
https://book.hacktricks.xyz/pentesting/pentesting-mssql-microsoft-sql-server
https://www.tarlogic.com/blog/red-team-tales-0x01/
https://pentestlab.blog/2013/03/18/penetration-testing-sql-servers/
https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
https://github.com/balaasif6789/AD-Pentesting
https://github.com/swisskyrepo/PayloadsAllTheThings
https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
https://github.com/infosecn1nja/Red-Teaming-Toolkit